

REMARKS

This communication is a full and timely response to the Office Action dated September 22, 2008. Claims 1-6 remain pending and claims 1-6 are rejected. By this communication, claims 1 and 3 are amended for clarity purposes. No claims are added or canceled.

Rejection Under 35 U.S.C. § 102

Claims 1-6 are rejected under 35 U.S.C. §102(e) for allegedly being anticipated by *Vetillard* (U.S. Patent Publication No. 2005/0107069). Applicants respectfully traverse this rejection.

Independent claim 1 of the instant application recites, in part, "downloading the signed original code and the signed software component into the card; and on card: verifying the signatures respectively of the original code and of the software component, and applying the software component to the original code so as to reconstruct the modified code for its execution by the microprocessor."

Contrary to the position taken by the Office, *Vetillard* fails to disclose or suggest at least the preceding claimed combination of features. *Vetillard* discloses a method and device for securing messages exchanged over a data transmission network between a server and a client, under the control of an authority that defines message exchange rules. The device is decentralized and consists of a representative 3 of the authority inserted permanently into the network between the server 1 and the client 2 during the secure exchange of messages. *Vetillard*, pg. 2, paragraph [0047] and Figure 1. The client 2 may be a data processing microsystem such as a smart card or some other onboard system with limited security capabilities. *Id*, pg. 2, paragraph [0057]. A dedicated smart may represent the verification

authority and may constitute the representative 3 of the authority. *Id*, pg. 3, paragraph [0058]. The representative 3 of the authority sets up two secure channels for exchanging messages: (1) a first secure channel 4, between the server 1 and the representative 3 of the authority, using a first key K_s known to the representative 3 of the authority and to the server 1 but not to the client 2, and using a first encryption algorithm AL, and (2) a second secure channel 5, between the representative 3 of the authority and the client 2, using a second key K_c known to the representative 3 of the authority and to the client 2 but not to the server 1, and using a second encryption algorithm AL'. *Id*, pg. 3, paragraphs [0059] - [0060] and Figure 2.

The server 1 sets up a first secure channel 4 with the representative 3 of the authority using the key K_s and the algorithm AL. The server 1 sends the code C to be loaded to the representative 3 of the authority via the first secure channel 4. The representative 3 of the authority verifies the properties on the code C (notated by 'VC'). The representative 3 of the authority sets up a second secure channel 5 with the client 2 using the second secure channel 5 as previously set. It therefore transmits $VC(AL')K_c$. *Id*, pg. 3, paragraph [0063] - [0067].

Thus, as discussed above, *Vetillard* teaches a method for securely exchanging data between a server and a client. In particular, the method allows for loading a program from the server to the client. According to *Vetillard*, a third element, i.e., representative of the authority, is placed between the server and the client. Both the representative of the authority and the client may be of smart card type. The representative of the authority is able to process data with two different keys, K_c and K_s . The representative of the authority and the server know the first key K_s . The client does not know the first key K_s (See *Vetillard*, page 3, paragraph

[0059]). As a consequence, the representative of the authority and the client are two distinct entities.

Further, *Vetillard* teaches a method in which a program is loaded in a smart card (e.g., client) by using a secure channel (using a second key Kc). The program (VC) has been encrypted using a specific algorithm AL' and the second key Kc. The client decrypts the program and then may use the decrypted program. According to *Vetillard*, only one element (i.e., the code VC) is loaded in the smart card (e.g., client). However, according to the method of the instant application, the signed original code and the signed software component are loaded in the smart card. In other words, two distinct elements are loaded in the smart card instead of one.

Moreover, in the instant application, a modified code is generated by applying the software component to the original code in the smart card. Both the original code and the modified code are executable by the smart card. However, in *Vetillard*, only one code is intended to be sent by the server and loaded into the client. As such, *Vetillard* is not able to resolve issues such as those discussed in the specification beginning at page 5, line 15.

Therefore, *Vetillard* does not disclose at least "downloading the signed original code and the signed software component into **the card**; and **on card**: verifying the signatures respectively of the original code and of the software component, and **applying the software component to the original code so as to reconstruct the modified code for its execution by the microprocessor**" as recited in independent claim 1. In rejecting claim 1, the Office Action refers to paragraphs 0058, 0059, 0073 and 0074 of *Vetillard* in connection with these claimed

features. However, it is not apparent how they can be interpreted to suggest these claimed features, nor does the Office action offer any explanation of such an interpretation.

The Office is reminded that to properly anticipate a claim, the reference must disclose, explicitly or implicitly, each and every feature recited in the claim. See Verdegall Bros. v. Union Oil Co. of Calif., 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). For at least the foregoing reasons, Applicants respectfully submit that the Office has not met its burden to establish a case of anticipation with respect to independent claim 1, nor the corresponding dependent claims. Accordingly, withdrawal of this rejection is respectfully requested.

Conclusion

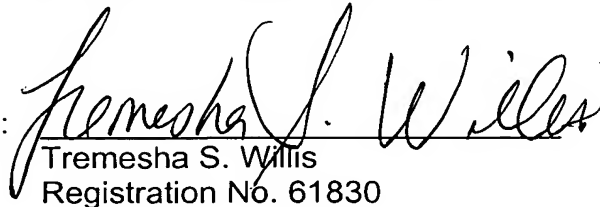
Based on at least the foregoing amendments and remarks, Applicants submit that claims 1-6 are allowable, and that this application is in condition for allowance. Accordingly, Applicants request a favorable examination and consideration of the instant application. In the event the instant application can be placed in even better form, Applicants request that the undersigned attorney be contacted at the number below.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: December 22, 2008

By:


Tremesha S. Willis
Registration No. 61830

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620